Surf's up! Protecting the privacy of health information on the Internet

We need new privacy laws and better encryption of information

Mark A Graber
Associate professor
Departments of Emergency Medicine and Family Medicine
University of Iowa College of Medicine
200 Hawkins Dr
PFP
Iowa City, IA 52242
mark-graber@uiowa.edu

Competing interests: None declared

West J Med 2002;176:79-81

The Internet is a ready source of medical information, but most patients do not realize that as they surf it, they leave behind information about themselves that creates a personal profile as unique as their DNA. This personal information becomes public knowledge that can be bought and sold by commercial interests. Physicians, too, are largely unaware that the e-mail messages they send to patients can be intercepted and that electronic medical records are also vulnerable to being accessed and can be distributed worldwide, once compromised.

It is a fallacy for patients to assume that the Internet protects their privacy. Every illness or drug name that they enter into a search engine is being tracked. Discussing their human immunodeficiency virus status in an online forum is the electronic equivalent of making a public announcement in a mall. Internet users are being

watched surreptitiously through a variety of technologies, such as "spyware," that is embedded in free games and that monitors what users download and what they run on their computer. Advertisements frequently contain code that tracks what people type when they are surfing the Internet and what kind of information they are looking at. Web sites can track what users are doing by using "cookies," small bits of information placed onto computers. And electronic "bugs" can send every word that Internet users type on their computer to a hacker; these bugs can be included in users' e-mail messages without their knowledge.

This is not just scare mongering. Although the US government insists on the privacy of medical records, such privacy is breached regularly.[1,2] Recent high-profile cases include the publication by Eli Lilly Company of the names of patients taking fluoxetine hydrochloride (Prozac),[3] the public posting of pediatric psychiatric information at the University of Montana,[4] and the hacking of 5,000 patient records at the University of Washington.[5] And this is only the tip of the iceberg.[5]

So we are left with a dilemma. How do we honor the privacy that users expect without limiting their access to health information on the Internet?[6] Present laws and assumptions are inadequate. The current laws, such as The Health Insurance Portability and Accountability Act of 1996, protect only a portion of online medical information.[7] We cannot assume that users are able to protect themselves (see, for example, the web site of WebSideStory, Inc, which states that it provides "e-business intelligence services").[8] The current steps being taken by some Internet sites to improve privacy, such as posting their privacy policies and offering users the ability to "opt out" of having their personal information shared, seem promising.[9] However, in one systematic study, 23% of commercial health sites did not post a privacy policy, and most written policies are incomprehensible to most users.[10,11] Even when they are present, privacy policies and opt-out clauses are no guarantee that a person's information is secure. Companies often violate their own privacy policies, rendering them useless.[12] In addition, because compliance is voluntary, there is no enforcement mechanism.[13]

John Schleith/©1998 The MITRE Corp. All rights reserved.

Privacy on the Internet remains elusive (Used with permission of The MITRE Corporation)

There are three possible solutions to the problem of protecting patients' electronic information. First, there should be a legally mandated "opt-in" policy for health information; this would require that users actively give permission for their online information to be distributed. This is the same protection that is given to other medical information. Current opt-out policies assume that most users would default to having their health information shared, which is not the case. Second, all electronic or web-based medical information should be encrypted. This can be done seamlessly so that it would be transparent to the intended user, and it would mean that unauthorized hackers would view only gibberish. Inadvertently released records would be unintelligible without the proper key. Current encryption schemes are up to the task; many require a sophisticated mainframe computer to break the encryption. Third, the release of protected electronic medical information should be made a criminal or civil offense. This would change the current paradigm by signaling that this information is of value and considered important enough to protect.

As advocates for patients, physicians should insist on the same level of protection for online medical profiles as is given to other confidential health information. In many cases, what is entered online contains the same level of detail as what is in an office record (see, for example, www.MDExpert.com or www.PersonalMD.com). A few simple steps would help. Physicians can inform patients that any information they provide while surfing the Internet is public knowledge. They can also encrypt their e-mail messages to patients or use any another technique to ensure e-mail security. Finally, physicians can make sure that their personal and office computers are protected. Hackers randomly attack thousands of computers at a time. These hackers can place a "trojan horse" (or other software) on a computer that allows them to come back and peruse the system at will. My home computer, which has a dial-up Internet connection, has been hacked into (and successfully defended) hundreds of times. If you use a high-speed cable modem or DSL that is always connected, your computer is at even more risk of being attacked by hackers. Computer security is not something that most computer users tend to themselves. However, a system administrator should be able to help. If physicians

Finding out more about privacy of electronic information

Sites with information about electronic privacy

- www.healthprivacy.org
- www.privacyfoundation.org
- www.understandingprivacy.org
- www.primers.net/security
- www.junkbusters.com
- www.grc.com

Sites with free or cheap tools for protecting privacy

- www.grc.com
- www.webwasher.com
- www.pgp.com
- www.zonelabs.com
- www.becky-users.morelerbe.com/spyblocker/

use their home computer to communicate with patients, they should make sure that it, too, is secure.

Many tools are available that will defeat the online tracking of personal information and that will maintain the integrity of computers and e-mail, and many are free or very inexpensive (see box).

We cannot and should not reverse the trend toward the computerization of medical information. However, as with previous industrial revolutions, technology has outpaced social evolution. Instead of being Luddites who smash power looms, physicians should insist that the rules of society catch up with the revolution in electronic medical information.

References

1 US Dept of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information, Rules and Regulations. 66 *Federal Register* 12434 (2001) (codified at 45 CFR §§160&164).
2 Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University. Medical Privacy Stories. July 2001. Available at www.healthprivacy.org/info-url_nocat2302/info-url_nocat.htm. Accessed December 3, 2001.
3 Yamey G. Eli Lilly violates patients' privacy [news]. *BMJ* 2001;323:65.
4 Piller C. Web mishap: kids' psychological files posted. *Los Angeles Times* November 7, 2001. Available at www.latimes.com/news/printedition/la-000088956nov07.story. Accessed December 5, 2001.
5 Health Privacy Project, Institute for Health Care Research and Policy. Georgetown University. July 12, 2001. Available at www.healthprivacy.org/usr_doc/mprivacystories%2Epdf. Accessed December 5, 2001.
6 Fox S, Rainie L, Horrigan J, Lenhart A, Spooner T, Carter C. *Trust and Privacy Online: Why Americans want to rewrite the rules.* The Internet Life Report. Pew Internet & American Life Project. August 20, 2000. Available at www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf. Accessed April 19, 2001.
7 Report of the Pew Internet & American Life Project, Health Privacy Project. *Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users.* November 2001. Available at www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=91796. Accessed December 5, 2001.
8 WebSideStory. Available at www.websidestory.com/cgi-bin/wss.cgi?corporate&news&press_2_124. Accessed April 19, 2001.
9 *Hearings Before the Senate Committee on Commerce, June 13, 2000, On Internet Privacy and Profiling.* (testimony of Richard M Smith). Available at www.senate.gov/~commerce/hearings/hearin00.html. Accessed April 19, 2001.
10 Graber MA, D'Alessandro DM, Johnson-West J. Is the reading level of privacy policies on Internet Health Websites too high for most users? *J Fam Pract*; in press.
11 Harris Interactive, for the Privacy Leadership Initiative. *Consumer Privacy Attitudes and Behaviors Survey, Wave III.* December 3, 2001. Available at www.understandingprivacy.org/content/library/harrissum12_01.pdf. Accessed December 5, 2001.
12 Goldman J, Hudson Z, Smith RM, for the California HealthCare Foundation. *Privacy: Report on the Privacy Policies and Practices of Health Web Sites.* January 2000. Available at admin.chcf.org/documents/ehealth/privacyexecsummary.pdf. Accessed December 5, 2001.
13 Choy A, Goldman J. *Comparing eHealth Privacy Initiatives.* November 2001. Available at ehealth.chcf.org/view/cfm?section=Privacy&itemID=4601. Accessed December 12, 2001.

ANY QUESTIONS?

Do you have a clinical question you'd like to see answered? If so, here's your chance to get a curbside consult from our expert team, which includes many of the top clinicians in the West.

ANY ANSWERS?

Maybe you have strong views about something you read in this issue—something we got wrong perhaps? Or do you have further clinical experience you'd like to share? Perhaps you have suggestions for new topics you'd like to see us address from an evidence-based perspective.

Whatever questions, comments, or other contributions you have, we'd like to receive them. We realize that it's experience like yours that makes the journal come alive. Please send your questions, ideas, or comments to us by email: wjm@ewjm.com.